# IMAGE CAPTURE METHOD, DEVICE AND SYSTEM

## Field of the Invention

**[0001]** The present invention relates to the field of image capture.

## Background to the Invention

**[0002]** Portable digital cameras have become miniaturized, and are becoming increasingly wide spread. Known mobile phone devices already have built in cameras, and picture messaging between mobile phones is an increasingly wide spread technology.

**[0003]** Further, wearable cameras are known, and have the potential for becoming widely used consumer products in the future.

**[0004]** For some persons, being included in photographs or picture messages when in public places has nuisance effect. Increasing usage of portable camera devices means that the privacy issue of capturing of images of subjects who would prefer not to be photographed has increased. Because portable cameras are small and are likely to be unseen by a subject, persons generally cannot choose to avoid being in the field of view of a small portable camera and are likely to have their pictures taken without their knowledge or consent.

**[0005]** The issue of privacy in relation to cameras is well known. Civil liberties organizations campaign for the right for people not to be photographed or videoed without their consent. However, with the widespread use of security cameras and other hand held portable camera devices, maintaining privacy from being photographed or videoed is becoming more difficult. Some security companies market their products as 'privacy friendly' because they are supposed

to retain only images containing faces of known individuals, typically, potential or actual criminals. In *'Privacy issues of wearable camera's –v- surveillance cameras'* by Steve Mann – HTTP//wearcam.org, 1995, it is suggested that security camera or wearable cameras should be made visible, and that a wearable camera should have a visual indicator that it is active for capturing an image. This does not offer actual privacy to individuals within the vicinity of the camera, but rather offers a chance to 'escape' from the field of view from a camera.

**[0006]** JP 10031265 discloses a device for preventing stealthy photographing in which a remote control receiver remotely controls a camera. The remote control receiver issues a warning sound when a camera captures an image. This does not prevent capture of a person's image, but rather alerts a person that a picture has been or could be taken.

**[0007]** Further, there are known security systems which are able to detect and identify faces of known criminals from security video footage, such as those available from Identix, and Viisage, for example the known FaceFINDER product.

**[0008]** US 20020039447 discloses a system for indexing, storage and retrieval of digital images, whereby photographs are sorted according to who is in a photograph, through face recognition algorithms.

**[0009]** US 20010016820 discloses a face identification system, whereby faces are removed from a memory device, having been identified.

**[0010]** JP 2001235812 discloses an image processing method and apparatus having a digital processing device with a masking pattern which can be superimposed on a portion of an image for obscuring that portion of the image. Control of the masking process lies with the operator of the photographic processing device. A person whose image has been captured by the device has

no control over the processing of the image or whether the image can be captured or not.

**[0011]** The ImageId company www.imageID.com has a known product, whereby a user wears a tag. The tags are recognized by cameras and used to sort out images of people. The product recognizes and reads a set of markings within an image, and then sorts and stores matching identification codes in a database.

**[0012]** US 6,067,399 discloses a privacy mode for cameras and camcorders. Images of persons' faces recorded on a camera or camcorder are detected and obscured. In US 6,067,399 the person whose image is being captured has no control over whether a privacy mode of a camera or camcorder apparatus is set or not. Instead, an operator of the camera/camcorder determines the privacy mode. Therefore, privacy is not in the control of a person whose image is being captured.

**[0013]** JP 2001313006, discloses a method and apparatus in which a person who does not wish to be photographed carried a portable device which emits infra-red light which 'floods' a sensor or film of a camera, thereby blanking the image. However, the method disclosed in JP 2001313006 disables image capture completely and inhibits all images being taken, within range of the device.

**Summary of the Invention**

**[0014]** According to one aspect a captured image of a scene is modified by a method and apparatus for detecting an inhibit signal emanating from an inhibitor device carried by a person within the scene. In response to the inhibit signal, (a) a portion of the image corresponding to the person is identified; and (b) the image of the scene is modified to obscure the image portion of the person.

**Brief Description of the Drawings**

**[0015]** For a better understanding of the invention and to show how the same can be carried into effect, there is now described by way of example only, specific embodiments, methods and processes according to the present invention with reference to the accompanying drawings in which:

**[0016]** Figure 1 is a schematic illustration of a first embodiment of an image capture system comprising an image capture device, and at least one inhibitor device for controlling operation of the image capture device for taking images of a host wearer of the inhibitor device;

**[0017]** Fig. 2 is a schematic illustration of an omni-directional communication link between an inhibitor device and an image capture device of the system of Fig. 1;

**[0018]** Fig. 3 is a schematic illustration of a second embodiment image capture system, in which a communication link uses a directional receiver beam between an image capture device and an inhibitor device in which the image capture device detects the inhibitor device;

**[0019]** Fig. 4 is a schematic illustration of the inhibitor device and camera device of Fig. 3, in which the image capture device points in a direction away from the inhibitor device;

**[0020]** Fig. 5 is a schematic illustration of a scenario of two inhibitor devices and a single image capture device, the inhibitor device being in a field of view of the image capture device;

**[0021]** Fig. 6 is a schematic illustration of an example of an image captured by an image capture device before image processing is applied;

**[0022]** Fig. 7 is a schematic illustration of the image of Fig. 6, after image processing is applied to modify the image taking account of inhibitor devices within a field of view of the image capture device;

**[0023]** Fig. 8 is a schematic illustration of components of one specific embodiment of an inhibitor device;

**[0024]** Fig. 9 is a schematic illustration of components of a specific embodiment of an image capture device;

**[0025]** Fig. 10 is a schematic illustration of a scenario in which an image capture device captures an image in a field of view which includes users wearing first and second inhibitor devices, and the image capture device recognizes one of the inhibitor devices;

**[0026]** Fig. 11 is a schematic illustration of processes carried out by an image capture device for recognizing an inhibitor device;

**[0027]** Fig. 12 is a schematic illustration of a signal processing channel within an image capture device;

**[0028]** Fig. 13 is a schematic illustration of a communication link between an image capture device and a remote third party, for obtaining authorization for decoding a portion of a captured image; and

**[0029]** Fig 14 is a schematic illustration of an image captured device, an inhibitor and a trusted third party.

**Detailed Description of the Drawing**

**[0030]** There is now described by way of example only specific embodiments of the invention. In the following description numerous specific details are set forth in order to provide a thorough understanding. It will be

apparent however, to one of ordinary skill in the art, that the present invention can be practiced without limitation to these specific details. In other instances, well known methods and structures have not been described in detail so as not to unnecessarily obscure the description.

**[0031]** In this document, the term 'scene image', relates to an electronic image of a scene, and includes both a still image, and a video sequence.

**[0032]** In this document, the term 'image capture device' relates to any device capable of capturing an image, and includes but is not limited to digital still cameras, and video cameras.

**[0033]** Specific embodiments relate to a person's image being made available to an image capture device, particularly although not exclusively a portable image capture device, without the consent of the person.

**[0034]** In one embodiment, a wearable device broadcasts an inhibit message to an area immediately surrounding a host wearer of the device. Any portable image capture devices, such as cameras or the like of third parties within range of the device receive the inhibit message, and in response to receiving the inhibit message, inhibit capture and/or apply processing of an image or part of an image.

**[0035]** Referring to Fig. 1 herein, there is illustrated schematically an inhibitor device 100 and an image capture device 101 in close proximity, in which the inhibitor device broadcasts an inhibit signal carrying an image capture inhibitor message. Camera device 101, picks up the signal carrying the inhibit message. On receiving the inhibit message, the image capture device reacts in various ways.

**[0036]** In one mode of operation, the image capture device 101 captures an image of a scene, which includes a host wearer of the inhibitor device 100. However, the image capture device 101 is unable to print or store a portion of the captured scene image which corresponds to a wearer of the inhibitor device 100. Data processing components within the image capture device 101 modify the scene image by (1) identifying areas of the scene image which relate to a person wearing inhibitor device 100, and (2) obliterating selected parts of the image of the wearer of the inhibitor device. The selected parts of the image which are obliterated typically comprise facial features, and also can include items of clothing.

**[0037]** Some specific embodiments described herein operate such that images which include people who prefer not to have their images captured are automatically and forcefully modified before viewing. In some embodiments the images are modified before storage, such that images of such persons are no longer recognizable in the captured image. Suitably, only the portion of an overall image which relates to a person who seeks privacy is obliterated from the image, leaving the remainder of the overall image intact.

**[0038]** The inhibitor device 100 sends an inhibit message either omni-directionally, or directionally. The image capture device 101 can receive one or more inhibit messages at the same time, either omni-directionally, or directionally.

**[0039]** The inhibit message sent by device 100 can be carried on a signal carrier including but not limited to an ultrasonic signal carrier; a microwave signal carrier; a radio frequency signal carrier; a visual light signal, or an infrared light signal.

**[0040]** In the second mode of operation an inhibit signal generated from a position within a field of view of image capture device 101 is identified, and its position within a capture image taken of that field of view is established. Having established the position of the inhibit signal within the field of view and its

position within a captured image, a portion of the image relating to a wearer of the inhibitor device is located. This can be done by device 101 using a pattern recognition algorithm. A suitable face detection algorithm is disclosed in *'Neural network based face detection'* Rowley, Baluga, Kanade, IEEE PAMI 20(1): pages 23-38. Capture device 101 identifies an image of a host wearer's face, device 101 can employ a further image-processing algorithm to obliterate or obscure details of the person's face. This can be done by reducing the resolution of the image corresponding to the person's face, or by blanking out that portion of the image, or any other like obliteration or obscuring method of the portion of the image.

**[0041]** In one specific embodiment, the inhibit message from device 100 is carried by an inhibit signal in the form of a physical light, or an infrared light. Such a light is detected by device 101 within the captured image, as a high intensity light spot. Device 101 thereby identifies within the image, the position of a wearer of the inhibitor device 101. In this embodiment, there is a line of sight view between the inhibitor device 100, and the image capture device 101.

**[0042]** In other embodiments, the inhibitor device 100 sends an ultrasonic signal, or a radio frequency signal or a microwave signal, in which case a line of sight between the image capture device 101 and the inhibitor device 100 is not essential, but the image capture device includes a receiver device to detect the energy emitted by the inhibitor device. The problem of device 101 locating the position of the inhibitor device 100 within a captured image needs to be addressed.

**[0043]** Fig. 2 includes an omni-directional pattern having circular -3dB level 200 associated with a signal transmitted by an inhibitor device 201. There is also shown an image capture device 202 having a receiver having an omni-directional pattern with a circular –3dB level 203. Since the inhibitor device 201 transmits omni-directionally and the image capture device 202 receives an inhibit message with an omni-directional receive pattern, whenever the inhibitor device

201 is within close enough range of the image capture device to receive the inhibit message, the image capture device 202 is inhibited.

**[0044]** However, in other embodiments, the image capture device and/or the inhibitor device have directional responses for sending and/or receiving an inhibit message.

**[0045]** Referring to Fig. 3 herein, there is illustrated schematically an inhibitor device 300 having an omni-directional pattern represented by a circular –3dB power level 301, and an image capture device 302 having a directional receive beam represented by an elongated –3dB level 303. When the image capture device 301 is pointing in a direction toward the inhibitor device 300, and device 301 is within range of being able to capture and recognize an inhibit message transmitted by the inhibitor device, the image capture device 301 is inhibited according to the modes described herein above.

**[0046]** In Fig. 4, the image capture device 302 and inhibitor device 300 of Fig. 3 are positioned so narrow beam 303 of the image capture device points away from the inhibitor device. Because the receive beam 303 of the image capture device 302 is directional, the image capture device is not inhibited even though the image capture device and inhibitor device may be in relatively close proximity. This is because the image capture device 302 points away from the inhibitor device 300 and device 302 has a narrow inhibitor receive beam that corresponds with the optical field of view of device 302.

**[0047]** In this embodiment, the directional beam 303 of the image capture device 302 correspond with an optical field of view of image capture of device 302, such that when the image capture device is pointing in a particular direction for capturing an optical image of a scene, the inhibit receive beam of the image capture device coincides with the optical field of view. Signals from inhibitor devices 300 which are outside the optical field of view of the image capture device 302 are not acted upon by the image capture device, so that the

image capture device is not inhibited by inhibitor devices 300 outside the optical field of view of device 302.

**[0048]** Fig. 5 is a schematic illustration of first and second inhibitor devices, 500, 501 respectively, worn by first and second persons (not shown) facing opposite to each other. Image capture device 502 is held or worn by a third person who is in the vicinity of the first and second persons wearing devices 500 and 501.

**[0049]** Each inhibitor device 500, 501 has a corresponding omni-directional antenna which produces a transmit pattern having a corresponding –3dB level 503, 504 respectively. Image capture device 502 has a receiver having a plurality of directional, relatively narrow inhibit receive beam patterns 505 to 509, pointing in different directions from each other and relative to a primary (front) look direction 510 of the optical image of image capture device. Beams 505 and 509 have axes displaced by approximately 70° to the left and right of direction 510, beams 506 and 508 have axes displaced by approximately 45° to the left and right of direction 50, and central beam 507 has an axis substantially aligned with direction 510.

**[0050]** The plurality of directional beams 505-509 enable the image capture device 502 to distinguish between the first and second inhibitor devices 500, 501 within a field of view of the image capture device, identified as being between straight line extremities 511, 512, that are equal angles relative to direction 510. The beam with inhibit pattern 503 from first inhibitor device 500 is received on central beam 507 and first left beam 506 of the image capture device 502, whilst a second inhibitor message on the beam with inhibit pattern 504 from second inhibitor device 501 is received on the center beam 507 and first right beam 508.

**[0051]** However if an operator of the image capture device 502 swings the image capture device so that the field of view points towards the inhibitor

device 500, then the directional receive beam 506 of the image capture device 502 receives a signal from inhibitor device 500, and the image capture device is inhibited according to the above described inhibited modes.

**[0052]** Processing steps carried out by an image capture device in a second mode of operation are described with reference to Figs. 6 and 7.

**[0053]** Figure 6 is a captured still image of a scene in which a primary subject of the image is a violinist. However, because the image is captured in a public place, a restaurant in this case, the background of the scene image includes images of two other persons.

**[0054]** A person capturing the image using an image capture device is likely to have no interest in the two diners in the background. However, in the absence of any mechanism for protection against capture of their images the two diners have no choice but to be included in the image scene. The person capturing the image can use the image for his own purposes, including putting the image publicly in the Internet, or otherwise publishing the image. This is likely to occur without the knowledge of the two persons whose images are in the background of the scene image. The persons included in the background of the image might object to being included in the image, if they had known the image had been captured.

**[0055]** Fig. 7 includes the same image scene as Fig. 6, but after data processing by an image capture device as described herein. The image of Fig. 7 was obtained as a result of the two diners wearing inhibit devices and the photographer using a capture device that has received inhibit messages from each of the diners in the background of the image scene.

**[0056]** The image capture device receives two inhibit messages, one from each inhibitor device, worn by each of the diners. In response to each inhibit message, the image capture device identifies a person wearing the

corresponding inhibitor device. The image capture device processes each frame of image data, to identify images of individual wearers of the inhibitor devices, and then applies data processing to obliterate or remove portions of the image relating to the individual wearers of the inhibitor devices.

**[0057]** Correlation of an inhibit signal to a person in an image can be done in several ways. According to one embodiment, using known face-recognition software (for example as mentioned supra), the face nearest to the perceived origin of the inhibitor signal is located in a reference frame defined by the image, and the located face mosaiced out of the image by processing circuitry included in the image capture device.

**[0058]** As shown in Fig. 7, this results in a blurring of the face of each of the diners in the resultant image frame, thereby protecting the identity and privacy of each of those persons.

**[0059]** A portion of the image scene corresponding to a person's face or other features of the person is inhibited by obscuring, restricting usage of, replacing and/or deleting the part of the image by various methods including, but not limited to the following:

**[0060]** Firstly, the image detector can decrease resolution of the facial image portion, so that facial features become blurred and difficult for a human eye to resolve with accuracy. The decreased resolution can be achieved by a digital filtering algorithm, which applies a decrease in resolution to the image portion corresponding to a facial feature of a person.

**[0061]** The image detector can alternatively identify a portion of the image by a known algorithm for detecting skin tone colours within the image scene. The portion of the image corresponding to a person's face is obscured by overlaying a pre-determined graphic on that portion of the image, to obscure or obliterate facial features or other body features of the person.

**[0062]** The image detector can alternatively de-focus a portion of the image scene corresponding to a person's face or other body features so that it is difficult visually for a viewer to resolve the image with any detail.

**[0063]** Another approach is for the image detector to obscure the image portion corresponding to the person's face or other body features by changing an intensity level of the image portion. Typically, the image portion is darkened to obscure facial features.

**[0064]** The image detector can also completely delete the facial or other body portion of the image and replace it with a different image, such as a duplicate of another adjacent portion of the image scene. For example, in the images shown in Figs. 6 and 7, a portion of the image scene corresponding to a person's face can be identified and removed from the image scene. The resulting gap in the image is replaced by an adjacent portion of the image scene, for example a background wall. The image detector overlays a wall on the gap of the image produced by removal of the image portion corresponding to the person's facial features or other body features. This has the advantage of retaining similar colouring as adjacent portions of the image.

**[0065]** Fig. 8 is a block diagram of components of an inhibitor device 800, corresponding to each of devices 100, 201, 300, 500 and 501. The inhibitor device 800 comprises a casing 801 containing a battery (not shown), a size and shape such that the casing easily worn by a person, or can be easily carried by a person, for example in the person's pocket. Casing 800 includes: (1) an inhibit message generator 802 for generating one or a plurality of inhibit message types; (2) a transmitter device 803 for transmitting one or more inhibit messages on a carrier signal; (3) an antenna 804 for generating an omni-directional inhibit transmit beam or one or a plurality of directional inhibit transmit beams; and a set of user controls 805 for enabling a person to turn the inhibitor device 80 on or off, and optionally for selecting an inhibit message type. Transmitter 803 is of any

suitable type, e.g.; RF, microwave, optical or sonic. The battery powers each of generator 802, transmitter 803, and user controls 805.

**[0066]** The inhibitor device 800 can also comprise a memory device capable of storing a plurality of images of a person's face, in a plurality of views or orientations, and be capable of transmitting the images either in encoded or in un-encoded format.

**[0067]** Fig. 9 is a block diagram of components of an image capture device 900, corresponding to each of devices 101, 202, 302 or 502. The image capture device 100 comprises a casing 901 containing a battery or other power supply and an antenna 902 for receiving inhibit messages from antenna 804. Antenna 902 has either an omni-directional receive beam, or one or plural directional receive beams. Device 900 also includes receiver device 903 for receiving, amplifying and digitising a signal from antenna 902. Direction finder 904 responds to the signal from receiver 903 for identifying the direction from which an inhibit signal includes on antenna 902 has been received, that is, for identifying from which one or more of a set of directional beams, an inhibit signal was received on. Direction finder 904 drives message recogniser 905 for extracting inhibit messages from received signals and interpreting the type of inhibit message received by antennae 902.

**[0068]** Device 900 includes a set of optics 906 for capturing an optical image in response to a user input signal. Imaging device 907 is coupled with optics 906 for converting the received light image of optics 906 into two dimensional image data as one or more image data frames, including still images and/or video sequences of a plurality of image frames. Imaging device 907 drives image memory 908 for processing image data frames that in turn selectively drives image data storage device 909 for storing captured images. Image processor 910 responds to message recogniser 905 to apply data processing to captured image data frames. The data processing that processor 910 performs is in accord with the various prior art techniques previously

described in connection with Figs. 6 and 7. Image capture device 900 also includes a set of user controls 911 for controlling capture of images via the imaging device 907, and for controlling other functions such as storage of images in the image data store 909, and for monitoring image processing of image data. Device 900 also includes an image viewer 912, for example a liquid crystal display (LCD) or the like, driven by imaging device 907 for viewing captured images. The antenna, receiver, direction finder, message recognizer and image processor constitute an image inhibitor module 913. The battery or other power supply in casing 901 powers electronic parts 903-905 and 907-912.

**[0069]** The inhibit signal transmitted by the inhibitor device 800 can be a visual signal, for example a red coloured visual signal emitted by a light emitting device at a wave length of approximately 633nm, or a green light emitted by an LED at a wave length of approximately 510nm, or may comprise an infrared signal or a microwave or RF frequency signal.

**[0070]** In various alternative embodiments, signal detector 901 and receiver 903 can be an optical detector, such as a photo diode, for detecting visual or infrared signals; an ultrasonic detector for detecting ultrasonic signals, or an antenna for detecting radio frequency signals.

Registration of inhibitor devices.

**[0071]** In a further modification of the image capture system described herein, individual inhibitor devices are registered with individual image capture devices, so as to override the normal inhibitor function of the inhibitor device with respect to those particular registered image capture devices. This function is useful in situations where inhibitor devices are worn by members of a family group, and one or more other members of the family group are carrying an image capture device. Persons within the family group may wish to have their image captured by their own family member, but want to prohibit capture of their images by other unknown third parties in a public place.

**[0072]** Fig. 10 is a schematic drawing of an image capture system, in which a plurality of inhibitor devices are pre-registered with one or more image capture devices, and in which the image capture device can ignore an inhibitor message emanating from a pre-registered inhibitor device. An image capture device 1000 receives first and second inhibitor message 1001, 1002 from first and second inhibitor devices 1003, 1004 respectively within a field of view of the image capture device. First inhibitor device 1003 sends an inhibitor message 1001 including a code which the image capture device 1000 recognises as denoting a known pre-registered inhibitor device. On the other hand, second inhibitor device 1004 sends a signal which is not recognised by image capture device 1000.

**[0073]** Fig. 11 is a flow chart of processes carried out by image capture device 1000 upon receiving an inhibit message, for checking whether the inhibit message relates to a pre-registered inhibitor device. During step 1100, the image capture device 1000 receives an input message. Device 1000 then, during step 1701, reads the message, and checks for an identification code. If device 1000 recognises the identification code as one which is pre-registered with the image capture device (step 1102), the image capture device advances to steps 1103 and ignores the inhibit message, and therefore takes no action to process parts of a captured image identified by the existence of the inhibit message. In other words, device 1000 does not modify any part of the image. However, if during step 1102, device 1102 does not recognize the identification code as one which is pre-registered with the image captured device, operation advances to step 1104, during which the image capture device 1000 restricts a portion of the image corresponding to the inhibit message in step 1104.

**[0074]** Consequently, for an image in a field of view where a plurality of inhibitor devices are present, some of which are recognised by the image capture device 1000 and some of which are not, the image capture device modifies portions of the image corresponding to inhibitor devices, which are not

recognised, and leaves un-modified portions of the image corresponding to inhibitor devices having recognised code.

**[0075]** Widespread usage of inhibitor devices can affect security cameras used in surveillance systems. In an environment such as a building society, bank, shop, gasoline filling station or the like public place, which are susceptible to criminal activity, criminals wearing inhibitor devices might inhibit a security camera to obscure details of the wearers' faces. Therefore, an embodiment includes a facility wherein an inhibit signal received by an image capture device can be overridden so that faces of wearers can be viewed. There are two main options for overriding the inhibit signal, that is (a) without the wearer's permission; and (b) with the wearer's permission.

**[0076]** A system wherein the inhibit signal can be overridden without the wearer's permission can be provided as a function built into the image capture device itself. However, building in such a function seriously compromises the privacy of wearers of inhibitor devices. In a more sophisticated embodiment, an operator of an image capture device can override an inhibit signal, only with permission of a trusted third party. In such a system, an operator of an image capture system sends an image to a trusted third party, having the modified image portions corresponding to a person's face, along with a request to reverse the obliteration of a specific person's facial features.

**[0077]** Fig. 12 is a flow diagram of a signal processing channel within an image capture device for storing a captured scene image in such a way that the image can only be viewed, stored or printed with personal details obscured of persons wearing inhibitor devices, but with a capability of obtaining a clear image of those persons with external authorisation from a third party.

**[0078]** In step 1200, image capture device 1000 captures an image scene simultaneously with receiving an inhibit signal during step 1201. During step 1202, device 1000 identifies a portion of the scene image which is restricted

by the inhibit signal. During step 1203 device 1000 encodes the identified portion of the image and then during step 1204 stores the image in an encoded format; encoding during step 1204 can include encryption, and protection with an encoding key. Therefore, if an encryption key is used device 1000 can only store inhibited portions of the image in an encrypted format under protection of the encryption key.

**[0079]** During step 1205, device 1000 processes the scene image so that inhibited portions of the scene are obscured or obliterated. The processed scene image, having portions of the image obliterated or obscured is then stored during step 1206, and/or made available for viewing or printing during step 1207.

**[0080]** Fig. 13 includes a communication network 1300 between an image capture device 1303 (in the form of a digital video camera) and a trusted third party computer 1301. Communication link 1304 is, for example, the Internet, for ascending an encoded image portion to a trusted computer authority 1301, for decoding, so that images of persons can be recovered from the encoded stored image portions under control of trusted authority 1301. When an operator of the image capture device 1303 wishes to obtain a clear image of a particular person who has inhibited capture of the image of the particular device using an inhibitor device, the user can only do so provided the trusted authority 1301 agrees to authorise production of a clear image portion free of the particular person. The operator of the image capture device 1303 cannot bypass the trusted authority 1301, since the stored image portions are encrypted, and can only be decrypted with a key available to an operator of the trusted authority.

**[0081]** Several further variations on the embodiments described herein can be incorporated as follows.

**[0082]** Fig. 14 is a schematic illustration of a system including inhibitor device 1600 and a digital video camera that comprises image capture device 1601, and a remote trusted third party computer 1602. An image of a host

wearer of inhibitor device 1600 is coupled to either an image inhibitor module (the same as module 913) within the image capture device 1601, and/or to a trusted third party computer 1602. The image is coupled to computer 1602 via a cellular telephone camera (not shown) that communicates with computer 1601 via a communicator network 1603 that can include a cellular phone network and the Internet. The image of the host wearer of the inhibitor device 1600 can be sent to computer 1602 either as a clear un-encoded image, or it can be sent as an encoded image, in order to prevent misappropriation of the image when it is being coupled between the person wearing inhibitor device 1600 and the image capture device 1601 or between the person wearing inhibitor device 1600 and the trusted third party computer 1602.

**[0083]** Image inhibitor device 1600 also transmits to an inhibit signal that is coupled to image capture device 1601 and/or computer 1602. Transmission of the inhibit signal from device 1600 to computer 1602 is via network 1603.

**[0084]** Operation of the image capture system of Fig. 14 is as follows. Image capture device 1601 captures an image of a scene in the optical field of view of the image capture device 1601. Within that scene, there may be one or more inhibitor devices 1600. The inhibitor devices 1600 announce their presence within the field of view to the image capture device 1601, by transmitting a recognition signal, which can be the inhibitor message as described previously with respect to the embodiment of Fig. 1. However, in addition to that message, the inhibitor device 1600 coupled to the image capture device 1601 an image of the host wearer. The image capture device 1601 matches that received image, with a portion of the image captured by the image capture device 1601, which corresponds to a host wearer of the inhibitor device 1600. Devices 1601 matches the image of the wearer of inhibitor device 1600 with a portion of the image scene captured by the image capture device 1601 by pattern matching or pattern recognition algorithms which match the host wearer's facial image with positions of the captured image scene to detect a match of profiles.

**[0085]** The image of the wearer of the inhibitor device 1600 sends to the image capture device 1601 may comprise several views of the face of the wearer of device 1600, so that the face can be recognised from a variety of different view angles.

**[0086]** In a further mode of operation of the embodiment of Fig. 14, the image(s) of the host wearer's face are sent to a trusted third party computer 1602 operated by an independent authority having responsibility for decoding portions of an image. The trusted third party computer 1602 uses the host wearer's image to recognize portions of a scene image which have been sent to the computer by image capture device 1601, to decode that part of the image as described previously with respect of the embodiment of Fig. 13. In this mode of operation, which has application for obtaining decoding of images taken by a security camera, the operator of the image capture device 1601 must obtain authorization to decode a portion of the image. The trusted third party computer 1602 uses the inhibit signal and the image of the wearer of device 1600, as received from network 1603, to decode an obliterated or modified portion of the scene image corresponding to the wearer's face, so that the operator of the image capture device 1601 can obtain from the trusted third party, a clear image of the host wearer's face.

Activation of the Image Inhibitor Module.

**[0087]** In a further variation of the embodiments described herein, activation of an image inhibitor device depends upon either the distance between an image capture device and an inhibitor device, or an effective resolution of an image which the image capture device can capture.

**[0088]** In the first case, an inhibitor device and/or an image capture device are provided with known distance measuring devices, for example a diode laser based measuring system as known in the art. The image capture device

measures the distance between itself and the inhibitor device within an optical field of view of the image capture device. In response to the distance measurement, the image inhibitor module of the image capture device is activated or de-activated. For inhibitor devices which are beyond a pre-specified range the image inhibitor module of the image capture device is deactivated, allowing the image capture device to store, print or display a scene image including an un-modified image of a host wearer's face. If the pre-specified distance is set correctly, the person will be so far in the distance, that the person will appear only as a small feature in the captured image, and it is difficult or impossible for persons examining that image to recognise the wearer of the inhibitor device due to the relatively small size of the image of the person as a proportion of the entire scene image.

**[0089]** In the second case, the image inhibitor module of the image sensor does not modify any image portions where facial features are not recognised due to the low resolution of the facial features. For example, this may be because the wearer of an inhibitor device is so far away from the image capture device within an optical field of view of that device or the field of view is so dark that the facial features of the viewer cannot be captured with a significantly high resolution such as to enable a person to recognise the wearer of the inhibitor device.

**[0090]** In a further variation, the inhibitor device worn by a person is in the same casing as an image capture device, to provide an image capture device performing the dual role of enabling a person to capture images of a scene, while the same time providing a degree of privacy to that person from having their image captured by other image capture devices. For example, the inhibitor device, and an image capture device having an image inhibitor module, can be incorporated in a single hand held device, for example a mobile phone, or still image camera, or hand held video camera device.

**[0091]** In a further variation, within the image capture system, individual security groups or levels of security can be implicitly or explicitly used to ensure that if a person carries an inhibitor device, it will still be possible for an authorised person, for example a family member, to be able to capture an image of the wearer of the inhibitor device.

**[0092]** By combining an inhibit message or inhibit signal with pattern recognition of facial features, that is, by comparing an image sent by the inhibitor device with portions of a scene image, a portion of a scene image relating to a wearer's face can be more accurately adjusted and finally located, and modified to obscure the facial details of that person.

**[0093]** Specific embodiments disclosed herein provide that a person who does not want his image to be captured can carry a portable device to communicate with one or more image capture devices, such as a camera, which that person may encounter, to inhibit those image capture devices from using images of the person. The image capture system is de-centralised, and need not rely on a centralised database of images of the person's face.